

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-30596

(P2003-30596A)

(43) 公開日 平成15年1月31日 (2003.1.31)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	D 5 B 0 3 5
G 0 6 F 9/46	3 4 0	G 0 6 F 9/46	3 4 0 A 5 B 0 5 8
G 0 6 K 19/07		G 0 6 K 19/00	N 5 B 0 9 8

審査請求 未請求 請求項の数 8 O L (全 12 頁)

(21) 出願番号 特願2001-213641(P2001-213641)

(22) 出願日 平成13年7月13日 (2001.7.13)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 受田 賢知

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 片山 国弘

東京都小平市上水本町五丁目20番T1号

株式会社日立製作所半導体グループ内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

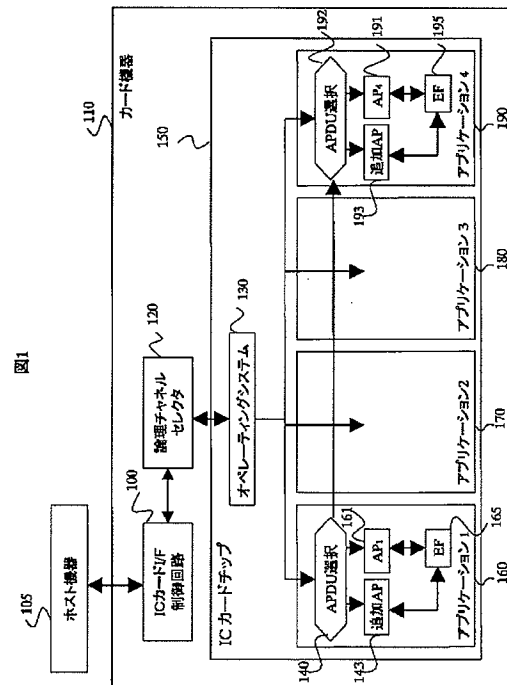
(54) 【発明の名称】 論理チャネル管理機能付き記憶装置

(57) 【要約】

【課題】 ICカードチップ及びICカード用オペレーティングシステムが論理チャネルの機能をサポートしていない場合には、ICカードチップ上で複数のアプリケーションを独立に、もしくは協調させて動作させることは難しい。

【解決手段】 本発明は、上記の問題を解決したものであり、ICカードインターフェイス制御回路とICカードチップ内に論理チャネルセレクタを挿入することにより、これとICカード内のアプリに挿入した追加アプリケーションとを用いて論理チャネルの機能を実現する。

図1



【特許請求の範囲】

【請求項1】データのセキュリティ処理を行う第1のメモリと、

前記第1のメモリを制御する制御装置と、

前記第1のメモリに論理チャネルの機能を付与する第2のメモリとを備えることを特徴とする記憶装置。

【請求項2】前記第2のメモリは、該記憶装置に接続されるホスト機器からの命令に論理チャネルに関する命令が含まれていた場合、前記論理チャネルに関する命令に対応する処理を実行する手段と、

前記ホスト機器から受信した命令の変換及び一つもしくは複数の命令を補完し、前記第1のメモリに送信する手段とを有する事を特徴とする請求項1記載の記憶装置。

【請求項3】請求項1記載の記憶装置であって、前記第1のメモリに入力される命令とは異なる体系の命令に対応する第3のメモリを有し、

前記第2のメモリは、該記憶装置に接続されるホスト機器からの命令に論理チャネルに関する命令が含まれていた場合、前記論理チャネルに関する命令に対応する処理を実行する手段と、

前記ホスト機器から受信した命令の変換及び一つもしくは複数の命令を補完し、前記第3のメモリに送信する手段とを有する事を特徴とする請求項1記載の記憶装置。

【請求項4】前記第2のメモリは、RAM及びEEPROMを有し、前記RAMに格納されたデータを前記EEPROMに書き込む第1のコマンドと、

前記第1のコマンドによって前記EEPROMに書き込まれたデータを前記RAMに書き戻す第2のコマンドと、

オペレーティングシステムによってアプリケーションを切り替える第3のコマンドとを用いて前記論理チャネルの処理を実行する手段とを有することを特徴とする請求項2記載の記憶装置。

【請求項5】前記第2のメモリは、前記ホスト機器からの命令に登録アプリケーションに関する命令が含まれていた場合、前記ホスト機器から送られてきた通常命令を擬似命令に変換する第1のモジュールと、

前記ホスト機器から送られてきたアプリケーション選択命令を擬似アプリケーション選択命令及び擬似アプリケーション選択終了命令に変換する第2のモジュールとを有することを特徴とする請求項4記載の記憶装置。

【請求項6】前記擬似アプリケーション選択命令は、前記第1のメモリに格納された第1のアプリケーションに対し、前記擬似アプリケーション選択命令によって指定された前記第1のメモリに格納された第2のアプリケーションの内部呼出を実行させる命令であり、

前記擬似アプリケーション選択終了命令は、前記第1のアプリケーションに対し、前記第2のアプリケーションの内部呼出を終了させる命令であることを特徴とする請求項5記載の記憶装置。

【請求項7】前記第1のアプリケーションは、コマンドが前記第1のメモリに格納された他のアプリケーションより送信されたものか、第2のメモリより送信されたものかを判断する手段と、

前記第2のメモリより受信したコマンドを処理する手段と、

前記第1のメモリにおけるその他のアプリケーションより受信したコマンドを処理する手段とを有することを特徴とする請求項6記載の記憶装置。

10 【請求項8】前記第1のアプリケーションは、前記第2のメモリより受信したコマンドを一つもしくは複数のコマンドに変換し、前記第2のアプリケーションに送信する手段を有することを特徴とする請求項7記載の記憶装置。

【発明の詳細な説明】

【0001】

20 【発明の属する技術分野】本発明は、セキュリティ機能を有する記憶装置及びその記憶装置を挿入可能なホスト機器及び記憶装置が挿入されたホスト機器に係り、特に、論理チャネルを管理するコントローラを有する記憶装置及びその記憶装置を挿入可能なホスト装置及びその記憶装置が挿入された端末装置に関する。

【0002】

【従来の技術】ICカードは、プラスチックカード基板中にIC（集積回路）チップを埋め込んだものであり、そのカードの表面にICチップの外部端子を持つ。ICチップの外部端子には、電源端子、クロック端子、データ入出力端子などが含まれている。ICカードは、ICカードと接続されるホスト装置から外部端子を介して電源や駆動クロックを直接供給されることによって動作する。ICカードは、外部端子を介してホスト機器との間で電気信号を送受信することにより、接続されたホスト機器と情報交換をおこなう。情報交換の結果として、ICカードは、計算結果や記憶情報の送出、記憶情報の変更をおこなう。ICカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。ICカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

【0003】

【発明が解決しようとする課題】ICカードチップに複数のアプリケーションが搭載される場合、論理チャネルをサポートしていないICカード又は、論理チャネルをサポートしていないICカード用オペレーティングシステムを搭載するICカードにおいては、同時に複数のアプリケーションを独立に、または協調させて動作させることは困難である。

50 【0004】また、ICカードに対する命令は、ISO/IEC 7816で規定された命令以外の命令を使用す

することも可能であるが、論理チャネルのシステムをICカード内のOSが操作する場合、ISO/IEC 7816で規定されない命令を用いると、同時に複数のデバイスを操作できるシステムである論理チャネルにおいて、ICカード内のアプリケーションしか操作できない。

【0005】本発明の目的は、ICカードに搭載された複数のアプリケーションを同時に独立して動作させることで、ICカードの利便性を向上することである。

【0006】

【課題を解決するための手段】上記の目的を達成するために、本発明は、データのセキュリティ処理を行う第1のメモリと、第1のメモリを制御する制御装置と、記憶装置に論理チャネルの機能を付与する第2のメモリを有する記憶装置とする。

【0007】さらに、第2のメモリは、記憶装置に接続されるホスト機器からの命令に論理チャネルに関する命令が含まれていた場合、論理チャネルの処理を実行してもよい。

【0008】さらに、第2のメモリは、RAM及びROMを有する構成としてもよい。この場合、更に第2のメモリは、RAMデータをEEPROMに書き込むコマンドと、EEPROMに書き込まれたデータをRAMにもどすコマンドと、オペレーティングシステムによってアプリケーションを切り替えるコマンドとを用いて論理チャネルの処理を実行してもよいさらに第2のメモリは、ホスト機器からの命令に登録アプリケーションに関する命令が含まれていた場合、ホスト機器から送られてきた通常命令を擬似命令に変換するモジュールと、ホスト機器から送られてきたアプリケーション選択命令を擬似アプリケーション選択命令、擬似アプリケーション選択終了命令に変換するモジュールとを有してもよい。

【0009】また、第1のメモリに格納されたアプリケーションは、コマンドが第1のメモリに格納された他のアプリケーションから送られてきたものか、第2のメモリから送られてきたものかを判断する手段と、他のアプリケーションから送られてきたコマンドを処理する手段と、第2のメモリから送られてきたコマンドを処理する手段とを有してもよい。

【0010】

【発明実施の形態】図1は、本発明を適用したカード機器110の構成を示す図である。カード機器110は、ICカードインターフェイス制御回路100、論理チャネルセクタ120、及びICカードチップ150から構成される。ICカードインターフェイス制御回路100は、ICカードチップ150の制御をおこない、ホスト機器105と論理チャネルセクタ120の間でコマンドAPDUの送受信を制御する。論理チャネルセクタ120は、ICカードチップ150及びICカードインターフェイス制御回路100とに接続され、論理チャネルをサポートしていないICカード及びICカード用

オペレーティングシステムに対し論理チャネル管理機能を提供し、コマンドAPDUを受け取る他の機器に命令を分配する。ここで他の機器とは、フラッシュメモリチップやRAM等が該当する。これらの機器に対応するコマンドAPDUは、必要ならば受け取ったコマンドAPDUを変換した後にこれらの機器を制御するコントローラに引き渡される。コマンドAPDUは、ISO/IEC 7816規格に準拠したICカード用の命令フォーマットおよびICカード用命令である。ICカードチップ150は、ICカードのプラスチック基板中に埋め込まれるマイコンチップである。ICカードチップ150が有する外部端子、電気信号プロトコル、及びコマンドは、ISO/IEC 7816規格に準拠している。ICカードチップ150の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子、グランド端子がある。ICカードインターフェイス制御回路100は、ICカードチップ150の外部端子からICカードチップ150にICカードコマンドを発行することによって、外部のホスト機器105から要求されたセキュリティ処理に必要な演算の実行を指示する。ICカードチップ150は、論理チャネルセクタ120と接続されている。尚、図1のICカードチップ150内に示された構成は、論理的な機能ブロックを示すものであり、物理的構成を示すものではない。

【0011】図5は、ICカードチップ150の内部の物理的構成を示す図である。ICカードチップ150は、演算処理をおこなうためのCPU（マイコン）520、データ（プログラムを含む）を記憶するためのROM（Read Only Memory）530、RAM（Random Access Memory）550、EEPROM（Electrically Erasable Programmable ROM）540、暗号/復号に関する処理をおこなうための暗号コプロセッサ560、及び外部装置とデータを送受信するためのシリアルインターフェース570とを有する。これらは、各々バス580によって接続される。ICカードチップ150は、暗号コプロセッサ560を用いて、ホスト機器105から送信されたコマンドAPDUに対応するセキュリティ処理を実行する。尚、暗号コプロセッサ560（ハードウェア）の代わりに、CPU520がプログラム（ソフトウェア）を用いてセキュリティ処理を実行してもよい。

【0012】ICカードチップ150は、複数のアプリケーションをROM530もしくはEEPROM540内に保存する。また、アプリケーションに固有のデータ領域をEEPROM530及びRAM550内に確保する。確保された各領域は、Fire Wallのような互いに干渉を許さない機構によって守られていることが望ましい。また、ICカードチップ150は、ICカードインターフェイス制御回路100から発行されたコマンドAPDUによりアプリケーション、データ、及び管理情報を登録及び抹消する。尚、アプリケーション等の登録、

抹消の処理は、アクセス認証によりその処理の実行の可否が決定されることが望ましい。また、ICカードチップ150は、ICカードインターフェイス制御回路100から発行されたコマンドAPDUによりアプリケーションの選択をおこなう機能を持つこともできる。

【0013】さらに、ICカードチップ150には、アプリケーションの選択機能を提供するオペレーティングシステムが搭載されていることが望ましい。このような機能を提供するオペレーティングシステムとしては、MULTOS (MULTOSはMondex Internationalの登録商標であり、MAOSCOコンソーシアムで仕様の決定及びライセンスの管理がおこなわれているマルチアプリケーション型ICカード用オペレーティングシステムである。) OS等が該当する。図1に示すオペレーティングシステム130はこのような機能を提供するもので、汎用のオペレーティングシステムでなくてもよい。

【0014】図1に戻って説明を続ける。オペレーティングシステム130は、コマンドAPDUを受け取ると、現在選択されているアプリケーション160に対し、送信されてきたコマンドAPDUを渡す。ただし、コマンドAPDUがアプリケーションの登録及び削除及び起動及び選択等のオペレーティングシステムで処理される命令の場合、オペレーティングシステム130がそのコマンドに対応する処理を実行する。アプリケーション160は、オペレーティングシステム130により送られてきたコマンドAPDUを判別し、アプリケーション固有の命令セット161又はアプリケーション共通の命令セット143に送る。アプリケーション共通の命令セット143とは、論理チャネルを実現する際に必要となる命令等を含む命令セット及びWIM命令セット等が該当する。アプリケーション固有の命令セット161及びアプリケーション共通の命令セット143は、鍵情報及び認証情報等が格納されたEF (Elementary File) 165へのアクセスが許されている。アプリケーション固有の命令セット161及びアプリケーション共通の命令セット143は、コマンドAPDUを受信すると、それに応じた処理をおこない、処理結果をホスト機器105に返す。

【0015】論理チャネルは、ISO/IEC 7816において規定されており、DF (Dedicated File) もしくはアプリケーションに論理的に独立なアクセス手段を提供する機能である。この機能により、ICカードは同時に複数のサービスを提供できる。しかし、オペレーティングシステムがこの機能を提供するには、オペレーティングシステムが動作するシステムの処理速度、メモリ容量が十分でなければならず、システムの機能等が制限されるICカードに用いられるオペレーティングシステムにおいては、論理チャネルが機能として提供されていない場合がある。このようなオペレーテ

ィングシステムとしてはMULTOS等が該当する。

【0016】図2は、論理チャネルセクタ120の内部構成を示した図である。論理チャネルセクタ120は、APDUセクタ210、論理チャネル管理モジュール220、APDU変換モジュール230、論理チャネル管理テーブル223を格納したRAM221、及びAPDU変換テーブル223を格納したEEPROM231内を有する。APDUセクタ210は、論理チャネル管理モジュール220及びAPDU変換モジュール230と接続され、ICカードインターフェイス制御回路100より受信したコマンドAPDUを判別し、適したモジュールに処理をおこなわせる機能及びICカード150からのレスポンスをICカードインターフェイス制御回路100へ返す機能を有する。論理チャネル管理モジュール220は、論理チャネルの予約及び解放をおこなう。RAM221には、現在利用されている論理チャネル番号、一度に開ける論理チャネル数、予約されている論理チャネル番号、現在開かれているアプリケーション番号、及びアプリケーション実行状況等が論理チャネル管理テーブル223として格納されている。論理チャネル管理モジュール220は、RAM221に格納された論理チャネル管理テーブル223の情報を利用して、論理チャネルの予約等の処理をおこなう。アプリケーションの実行状況とは、電源投入以後にどのアプリケーションが実行されたかについての情報である。

【0017】APDU変換モジュール230は、ICカードインターフェイス制御回路100から送られてきたコマンドAPDUの内、アプリケーションの切り替えに関するものについて、論理チャネルの機能を実現するために必要ならば1個以上のコマンドAPDUを送られてきたコマンドAPDUに補完してICカードチップ150に送信する機能を持つ。この一連のシーケンスの中でエラー等が発生した場合、APDU変換モジュール230は、シーケンス処理を中止し、ICカードインターフェイス制御回路100にその旨を伝える。EEPROM231には、コマンドAPDUに対応した一連のシーケンスがAPDU変換テーブル233として格納されており、APDU変換モジュール230は、APDU変換テーブル233の内容に基づき変換をおこなう。ただし、APDU変換の機能が一義的に実現できる場合、EEPROM231にこれらの情報を格納しなくても良い。APDU変換テーブル233を書き換えるために、専用のコマンドAPDUを用意してもよい。また、この書き換えにICカードチップ150のセキュリティ処理を利用してもよい。APDU変換テーブル233は、入力のコマンドAPDUによってその処理が指示されており、論理チャネルセクタ120が規定する方法で書き換えられる。例えば、APDU変換テーブル233が、入力のコマンドAPDUに応じたディレクトリ構造をとると

き、APDU変換テーブル233の書き換えは、対応するディレクトリの書き換えに相当する。

【0018】図3及び図4は、論理チャンネルの予約及び複数の論理チャンネルを用いてホスト機器105からアクセスが行われた場合の処理を示すフローチャートである。ICカードインターフェイス制御回路100からコマンドAPDUを受信する(311)と、論理チャンネルセクタ120は、コマンドAPDUが論理チャンネル予約命令かどうかを判断する。論理チャンネル予約命令はISO/IEC7816におけるMANAGE CHANNEL open命令に相当するICカード用命令である(331)。論理チャンネル予約命令の場合、論理チャンネル管理モジュール220は、論理チャンネル管理テーブル223を参照し、論理チャンネルにまだ空きがあるかどうかを判断する(333)。論理チャンネルに空きがあるなら、論理チャンネルセクタ120は、空いている論理チャンネルのうち0を除く一番若い番号をICカードインターフェイス制御回路100に送信する(337)。空いている論理チャンネルがない場合には、論理チャンネルセクタ120は、エラー信号に論理チャンネルが開けない旨をセットし、ICカードインターフェイス制御回路100に送信する(335)。ICカードインターフェイス制御回路100は、受信した値をホスト機器105に送る(313)。コマンドAPDUが論理チャンネル予約命令でないなら、論理チャンネルセクタ120は、論理チャンネル解放命令かどうかを判断する。論理チャンネル解放命令とはISO/IEC7816におけるMANAGE CHANNEL close命令に相当するICカード用命令である(339)。論理チャンネル解放命令の場合には、論理チャンネルセクタ120は、コマンドAPDUで指定された論理チャンネルが予約されているかどうかを判断する(341)。予約されている場合は、論理チャンネルセクタ120は、論理チャンネル管理テーブル223から指定された論理チャンネルを削除し、ICカードインターフェイス制御回路100に送信する(345)。論理チャンネルが予約されていない場合には、論理チャンネルセクタ120は、その旨をエラーとして通知する(343)。命令が論理チャンネルの予約とも解放とも異なる場合には、通常命令と判断される(431)。

【0019】接続されている機器がICカードチップ150のみの場合、論理チャンネルに関しない命令はICカードチップ150へと送信される。カード機器110にICカードチップ150、ICカードインターフェイス制御回路100、及び論理チャンネルセクタ120以外にコマンドAPDUを受けて動作する機器が搭載されており、かつ論理チャンネルセクタ120が受信したコマンドAPDUが論理チャンネルセクタ120に登録されている場合、論理チャンネルセクタ120は追加機器命令に関するコマンドAPDUを、追加された機器に送信してもよい。また、追加された機器に通常命令を送信

し、追加機器命令をICカードチップ150に送信してもよい。ここで通常命令とは、論理チャンネル管理に関する命令と追加機器命令以外の命令を指し、追加機器命令とは、論理チャンネルセクタ120に登録された命令を意味する。登録された命令の場合、論理チャンネルセクタ120は、他の機器が接続されているかどうかを確認し(449)、存在していないならば(451)、その旨をホスト機器105に送信する(411)。他の機器が接続されている場合、論理チャンネルセクタ120は、その機器にコマンドAPDUを送信する(453)。この時、他の機器に論理チャンネルセクタ120が含まれているならば、コマンドAPDUを分配し、別の機器へ送信してもよい。他の機器にコマンドAPDUを送信する場合、これらの機器も論理チャンネルにより管理されていることが望ましい。

【0020】コマンドAPDUが登録された命令でない場合、論理チャンネルセクタ120は指定された論理チャンネルが現在選択されているものかどうかを判断する(433)。指定された論理チャンネルが現在選択されている論理チャンネルの場合、論理チャンネルセクタ120は、コマンドAPDUをICカードチップ150に転送する(435)。ただし、コマンドAPDUがSELECT APPLICATION命令で、既に他の論理チャンネルによって使用されている場合は、エラーを返す。通常、アプリケーションは複数の論理チャンネルによって同時に実行されることが望ましいが、アプリケーション及びホストアプリケーションがこれを認めるならばその限りではない。ICカードチップ150は、このコマンドAPDUを解釈し、実行する(481)。指定された論理チャンネルが現在選択されているものでない場合、論理チャンネルセクタ120は、指定されたアプリケーションがはじめて選択されたものであるかどうかを判断する(437)。この場合、論理チャンネルセクタ120は、SELECT APPLICATION命令を送信し(439)、ICカード150側でコマンドAPDUの処理が行われる(483)。その後、論理チャンネルセクタ120は、受信したコマンドAPDUをICカードチップ150に転送し(447)、コマンドAPDUの処理がおこなわれる(491)。アプリケーションが既に選択されたものである場合には、論理チャンネルセクタ120は、WRITE STATIC命令(441)、SELECT APPLICATION命令(443)、READ STATIC命令(445)を順に発行し、ICカードチップ150は、これらを順に処理する(485、487、489)。WRITE STATIC命令とは、ICカードチップ150の現在指定されたアプリケーションが保持する一時データをEEPROM540に書き込むための命令であり、READ STATIC命令とはWRITE STATIC命令でEEPROM540に保存されたRAMイメージをRAM550に書きもどす命令である。ただし、ICカードインターフェイス制御回路100より発行された命令がSELECT APPLICATION命

令の場合は、ステップ447の処理を省略する。アプリケーションは各コマンドAPDU処理前後これら命令に該当する処理をおこなっても良いが、この手法を用いた場合、ICカードチップ150をより効率よく管理できる。この後、論理チャネルセクタ120は、受信したコマンドAPDUをICカードチップ150に転送し(447)、処理する(491)。ICカードインターフェイス制御回路100より受信したコマンドAPDU以外のコマンドAPDUに関する応答は、ICカードインターフェイス制御回路100に送信されず、論理チャネルセクタ120により処理される。エラーが発生した場合には、論理チャネルセクタ120は、受信したコマンドAPDUの応答として、内部で生成したエラーコードを、必要ならば変換をおこなった後にICカードインターフェイス制御回路100に返す。

【0021】論理チャネルセクタ120の位置は、ICカードチップ150とICカードインターフェイス制御回路100の間に限らない。論理チャネルセクタ120は、入力コマンドAPDUであり、出力コマンドAPDUであるような任意の場所に配置することができ、コマンドフォーマットが異なるが互換性がある場合にはコマンドフォーマットの変換をおこなって用いても良い。この場所は、ホスト機器105内、もしくはホスト機器105とカード機器110の間に挿入される、通信プロトコルもしくはコネクタ形状等の変換をおこなうカードリーダー等が該当する。また、複数のカード機器110を論理チャネルによって管理したい場合には、ホスト機器105に論理チャネルセクタ120を設置するのが望ましい。

【0022】通常、ICカードチップ150に格納されたアプリケーションは、論理チャネルを利用して独立に外部機器とアクセスをおこなうが、耐タンパ領域であるICカードチップ150の外部にデータを出すことなくアプリケーション間のデータ通信をおこないたい場合がある。これは、具体的には、電子財布の機能を持つアプリケーションに蓄えられた電子マネーの入金及び出金等の処理が該当する。

【0023】図6は、上述した処理を実現する際のフローチャートである。以下、図1の記載も引用しながら説明をおこなう。図4のステップ433において現在選択されている論理チャネルとは違う論理チャネルが選択された場合、論理チャネルセクタ120は、次にそれが登録アプリケーションの選択かどうかを判断する(611)。登録アプリケーションの選択でなかった場合、ステップ437以下のステップが実行される。登録アプリケーションの場合には、論理チャネルセクタ120は、ICカードチップ150の現在選択されているアプリケーション160に対して擬似アプリケーション選択命令を発行する(613)。擬似アプリケーション選択命令は、ホストから発行されたアプリケーション選択命

令(ISO/IEC 7816におけるSELECT APPLICATION命令に相当する)をICカードチップ150内の個々のアプリケーションが解する形式に変換する命令である。通常の利用においては、アプリケーション選択命令は個々のアプリケーションが処理するのではなくオペレーティングシステムのようなアプリケーションを制御するシステムが受信し実行するのが望ましい。しかし、アプリケーションの内部呼出をおこなう場合、アプリケーション選択命令はオペレーティングシステムをバイパスさせアプリケーションに送信できるほうがよい。本発明はこの機能を提供する。

【0024】アプリケーション160は、この命令を受け取ると、アプリケーション内部呼出命令に変換し、アプリケーション190を呼び出す(651)。呼び出されたアプリケーション190は、自分が内部呼出をされたかどうかを判断する(681)。内部からの呼び出しの場合は、内部呼出用APDU処理をおこない(683)、外部からの呼び出しの場合は外部呼出用APDU処理をおこなう(685)。アプリケーション190は、自らの呼び出しが内部からの呼び出しなのか外部(オペレーティングシステム130)からの呼び出しなのかを判断し、処理を分ける機能を持つ。また、擬似アプリケーション選択命令に対し、これを受け付けるかどうかの判断をする。この機能により、アプリケーション間でどのように通信をおこなうかを定める。例えば、通常のアプリケーションは内部呼び出しを受け付けられないように設定されていることが望ましい。また、電子マネーのようなアプリケーションは電子マネーアプリケーションに登録されたアプリケーションからしか呼び出されないように設定されていることが望ましい。

【0025】擬似アプリケーション選択命令以下の通常命令(615)は、アプリケーション160を介してアプリケーション190に送信されて(653)処理される(687)。具体的には、内部呼出命令を用い、送られてきた通常命令のフォーマットを変換し、呼び出す。内部呼出は他のアプリケーションが選択されるまで有効である。また、擬似アプリケーション選択命令を契機にして、ホスト機器105は、アプリケーション160及びアプリケーション190間で一つもしくは複数の処理をおこなうようなコマンドAPDUを発行してもよい。これにはアプリケーション間の認証や、電子マネーを用いた電子チケット等の商品の購入をおこなう操作等が該当する。

【0026】アプリケーション選択命令が発行された場合で、選択されたアプリケーションが呼び出し側のアプリケーションの場合(617)、RETURN命令を発行する(619)。呼び出し側アプリケーションは、これを機に内部呼び出しを終了し、以降に受信した命令はアプリケーション160用の命令として処理する。他のアプリケーションが選択された場合(621)は、RE

TURN命令を送信し(623)、呼び出しの終了をおこない(657)、次にWRITE STATIC命令(625)、SELECT APPLICATION命令(627)、READ STATIC命令(619)を順に発行し、処理をおこなう(659、661、689)。呼び出しの処理は入れ子構造になってよい。その際、オペレーティングシステム130及びICカードチップ150の制約によりRAMの容量が十分に確保できない、並びにアプリケーション切り替え時において、前に選択されていたアプリケーションに関する一時データ及びレジスタが保持されない等の場合には、アプリケーションを呼び出す前にこれらデータをEEPROM540に退避させ、アプリケーションの再呼び出し後、EEPROM540に退避した一時データ及びレジスタを復元させる。ただし、指定したアプリケーションにおいて内部呼出が認められていない場合には、内部呼出処理をおこなうことはできず、外部呼出として処理される。またこのとき、外部呼出しをおこなわずエラーを返してもよい。

【0027】論理チャネルの機能はICカードチップ150以外にも適用できる。これにはMultiMediaCard(「MultiMediaCard」はInfineon Technologies AGの登録商標である)や論理チャネルのサポートを利用する他のシステム等が該当する。また、デバイスの一つとしてICカードチップ150を利用しない場合、論理チャネルセクタ120へ送り、論理チャネルセクタ120が発行する命令のフォーマットは、ISO/IEC7816で規定されたICカード用命令のコマンドAPDUフォーマット以外を利用してもよい。ただし、コマンドセットがICカード用命令と互換性を持ち、かつICカード命令及び応答に変換可能な命令フォーマットを持つなら、論理チャネルセクタ120とICカードチップ150の間に命令変換装置を挿入することにより、ICカードチップ150を利用することもできる。また、APDU選択モジュール140及び192と論理チャネルに関する命令等、複数のアプリケーションにおいて共通の処理をおこなう場合、この機能をオペレーティングシステム130に該当するシステムが実装してもよい。

【0028】図7は、携帯端末等のホスト機器105及びSIMカード等のカード機器710を用い、WAP(Wireless Application Protocol)のサービスをおこなう例を示した図である。カード機器710は、セキュリティ処理をおこなうWIM(WAP Identity Module)として動作する。WAPとは、ワイヤレス通信ネットワーク上でサービスをおこなうアプリケーションのために、WAP forumにおいて定められた仕様であり、WIMとはWAP上でセキュリティ処理をおこなうアプリケーションのために定められた仕様である。ICカードチップ150内のアプリケーション760は、WIMアプリケーションを実行する機能を持ち、これはアプリケーション760内のAPDU選

択モジュール140により、WIM用命令743、アプリケーション選択関連命令、及びアプリケーション命令161に分けられる。ただし、アプリケーション選択関連命令はWIM用命令743の拡張セットとして含まれるものとする。また、アプリケーション790を電子マネーのためのアプリケーションとすると、アプリケーション790は、アプリケーション790に登録された他のアプリケーション770等に対し、アプリケーション790内のEEPROMに格納された電子マネーデータを増減する機能を持ち、このときおこなわれたやり取りをログとして上記EEPROMに保存する機能を持ち、また銀行などのアプリケーション790を発行した業者により上記ログを読み取り及び消去をおこなう機能と電子マネーデータを増減する機能を持つ。アプリケーションの内部呼出を利用することにより、電子マネーデータなどの秘密情報を外部に出すことなく処理をおこなうことができる。

【0029】図8は、MultiMediaCard(以下MMC)820内にICカードチップ150とフラッシュメモリチップ860を搭載し、これらを論理チャネルセクタ120によって制御する場合を示した図である。コントローラチップ850は、MMC外部端子830を制御するMMCインタフェース制御回路853、ICカードチップ150の制御をおこなうICカードインターフェイス制御回路100、フラッシュメモリチップ160の制御をおこなうフラッシュメモリ制御回路855、論理チャネルセクタ120、及びこれらを制御するコントローラモジュール857から成る。フラッシュメモリチップ860は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きがなされる。MMC外部端子830は7つの端子から構成され、外部のホスト機器105と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。ホスト機器105は、一つ又は複数のフラッシュメモリ用の論理チャネルとその他のICカード用の論理チャネルを持ち、それらは論理チャネルセクタ120により切り替えられ、それぞれのコントローラに送られる。この仕組みを用いることにより、互いに独立にもしくは協調してフラッシュメモリとICカードのアクセスをおこなうようなアプリケーションを実現する。この仕組みによりICカードチップ150へのアクセスとフラッシュメモリチップ860へのアクセスの仕組みを共通化できる。またこの仕組みはICカードチップ150をコントローラチップ850内に含めた構成をとる場合にも有効である。

【0030】

【発明の効果】本発明によれば論理チャネルをサポートしないICカード及びICカード用オペレーティングシステムに対し、論理チャネルの機能を付与することで、ICカードの利便性を向上するという効果を奏すること

ができる。

【図面の簡単な説明】

【図1】 ICカードチップを有するカード機器の内部構成をあらわす図である。

【図2】 論理チャンネルセクタの内部構成をあらわす図である。

【図3】 論理チャンネル管理の手順を示すフローチャートである。

【図4】 論理チャンネル管理の手順を示すフローチャートである。

【図5】 ICカードチップの内部構成をあらわす図である。

* 【図6】 アプリケーションの内部呼出をおこなう際のフローチャートである。

【図7】 ICカードチップを有するカード機器を用いてWAPのサービスをおこなう際の内部構成をあらわす図である。

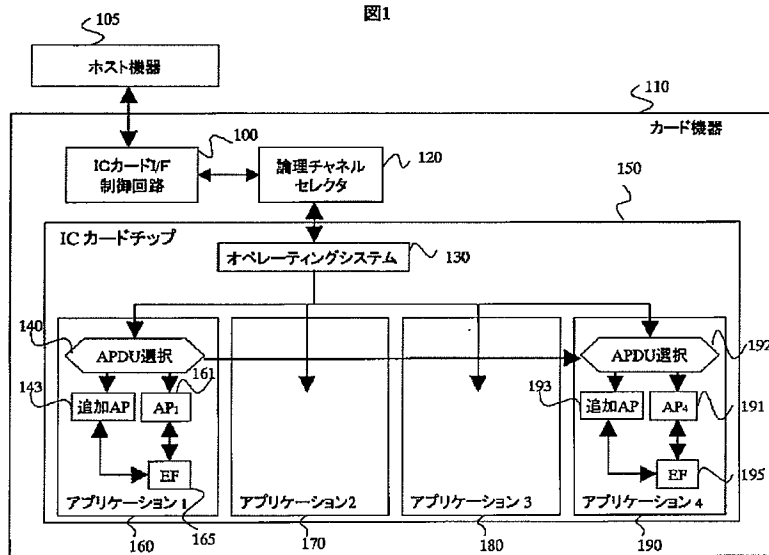
【図8】 ICカードチップを有するMMCに論理チャンネルセクタを搭載した場合をあらわす図である。

【符号の説明】

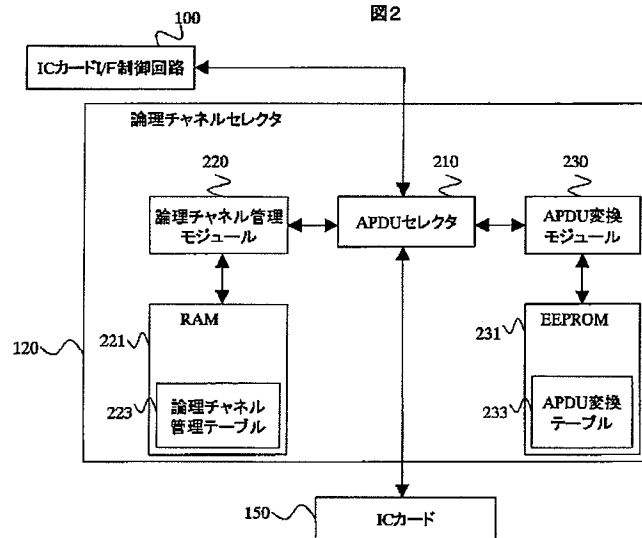
105…ホスト機器、100…ICカードインタフェース制御回路、120…論理チャンネルセクタ、150…ICカードチップ。

*

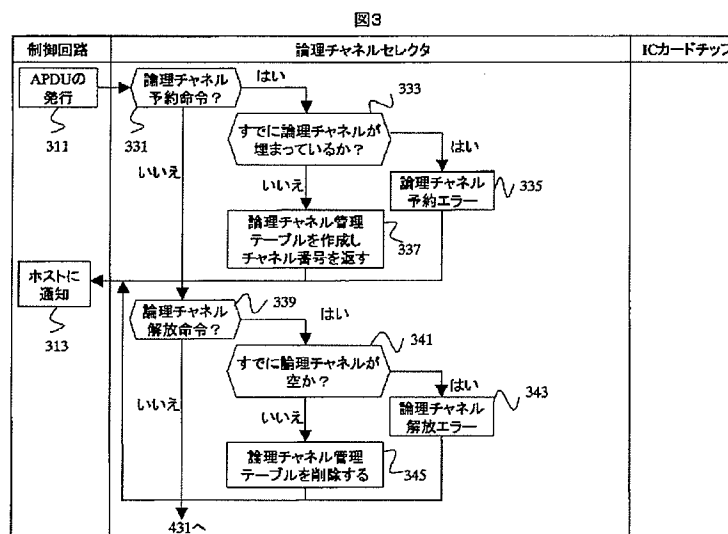
【図1】



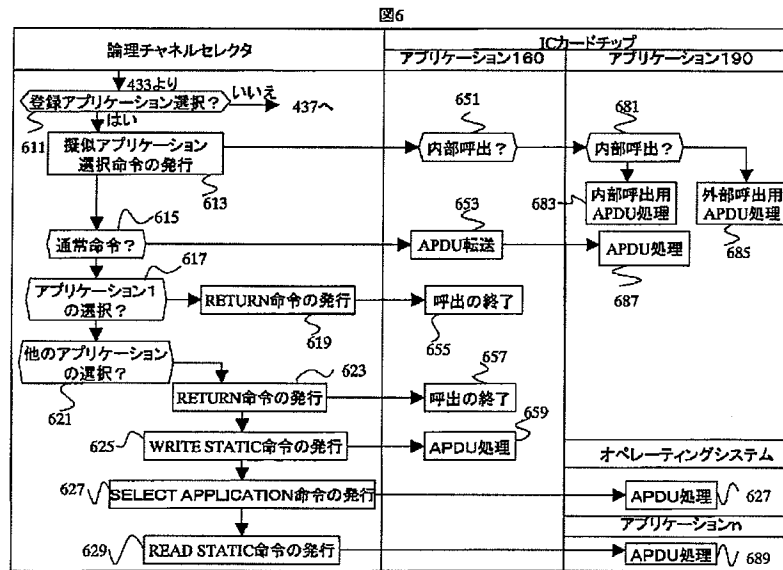
【図2】



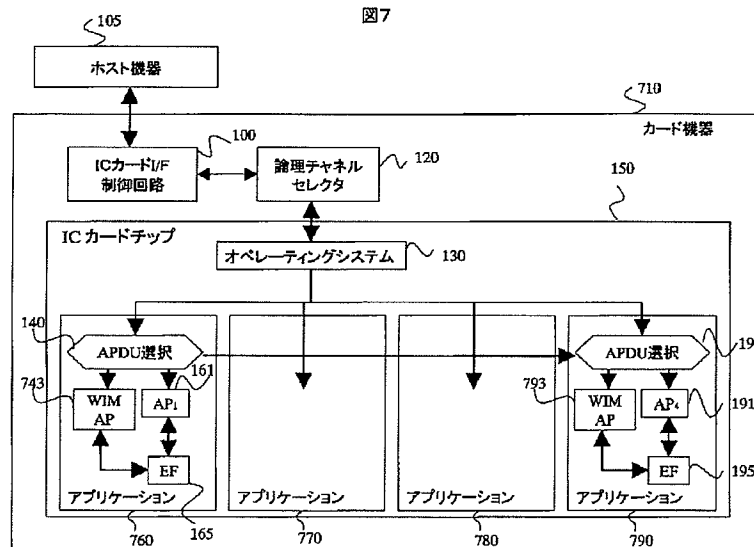
【図3】



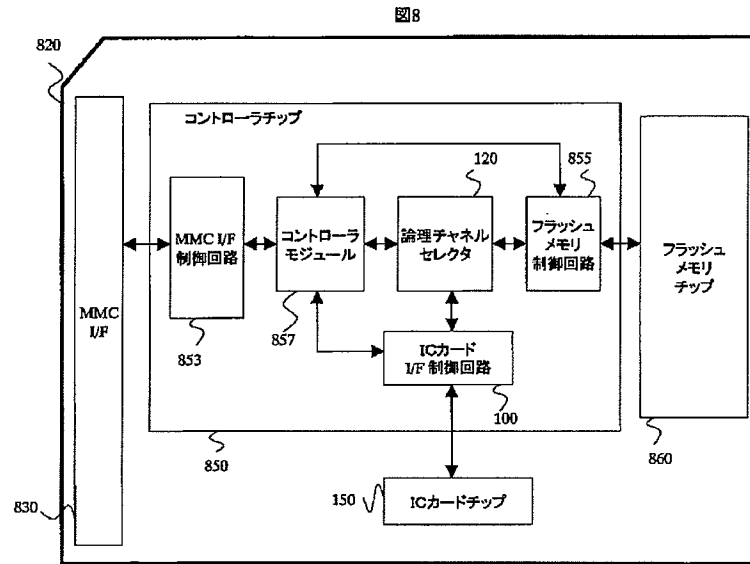
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 幡野 富久
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
(72)発明者 角田 元泰
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 水島 永雅
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
F ターム(参考) 5B035 AA06 BB09 CA29
5B058 CA23
5B098 GA02 GA07 GC01

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the host equipment in which the host equipment which can insert the memory storage which has a security function, and its memory storage, and memory storage were inserted, It is related with the terminal unit with which the host device which can insert the memory storage which has a controller which manages a logical channel especially, and its memory storage, and its memory storage were inserted.

[0002]

[Description of the Prior Art]An IC card embeds IC (integrated circuit) chip into a plastic card board, and has an external terminal of an IC chip in the card-face side. A power supply terminal, a clock terminal, a data input/output terminal, etc. are contained in the external terminal of an IC chip. The IC card operates by carrying out direct supply of a power supply or the driving clock via an external terminal from the host device connected with an IC card. An IC card exchanges information with the connected host equipment by transmitting and receiving an electrical signal between host equipment via an external terminal. As a result of information exchange, an IC card performs sending out of a calculation result or memory information, and change of memory information. The IC card can have the function to perform security processings, such as security data protection and personal authentication, based on such operation specifications. In the system for which the security of extra sensitive information, such as credit settlement and banking, is needed, the IC card is used as a user device for identification.

[0003]

[Problem to be solved by the invention]The IC card which is not supporting the logical channel when two or more applications are carried in IC card chip. Or in the IC card which carries the operating system for IC cards which is not supporting the logical channel, it is difficult to make

two or more applications cooperate and to operate them independently, simultaneously.

[0004]Although it is also possible to use commands other than the command specified by ISO/IEC7816, the command to an IC card, If the command which is not specified by ISO/IEC7816 is used when OS in an IC card operates the system of a logical channel, only the application in an IC card can be operated in the logical channel which is a system which can operate two or more devices simultaneously.

[0005]The purpose of this invention is to operate simultaneously independently two or more applications carried in the IC card, and is improving the convenience of an IC card.

[0006]

[Means for solving problem]In order to attain the above-mentioned purpose, let this inventions be the 1st memory that performs security processing of data, a control device which controls the 1st memory, and the memory storage which has the 2nd memory that gives the function of a logical channel to memory storage.

[0007]The 2nd memory may perform processing of a logical channel, when the command about a logical channel is included in the command from the host equipment connected to memory storage.

[0008]The 2nd memory is good also as composition which has RAM and ROM. In this case, the command by which the 2nd memory writes RAM data in EEPROM, processing of a logical channel may be performed using the command which returns the data written in EEPROM to RAM, and the command which changes application with an operating system -- to a pan the 2nd memory, The module which has been sent from host equipment when the command about registration application is included in the command from host equipment and which usually changes a command into a pseudo-instruction, It may have a module which changes into a false application selection command and a false application selection end instruction the application selection command sent from host equipment.

[0009]The application stored in the 1st memory, A means by which a command judges what has been sent from other applications stored in the 1st memory, and the thing sent from the 2nd memory, It may have a means to process the command sent from other applications, and a means to process the command sent from the 2nd memory.

[0010]

[An invention embodiment] Drawing 1 is a figure showing composition of the carding machine machine 110 which applied this invention. The carding machine machine 110 comprises the IC card interface control circuit 100, the logic channel selector 120, and the IC card chip 150. The IC card interface control circuit 100 controls the IC card chip 150, and controls transmission and reception of the command APDU between the host equipment 105 and the logic channel selector 120. The logic channel selector 120 is connected to the IC card chip 150 and the IC card interface control circuit 100, A logical channel controlling function is provided to an

operating system for an IC card and IC cards which is not supporting a logical channel, and a command is distributed to other apparatus which receives the command APDU. A flash memory chip, RAM, etc. correspond with other apparatus here. After the command APDU corresponding to these apparatus changes the command APDU received when necessary, it is handed over by controller which controls these apparatus. The command APDU is a command format and a command for IC cards for IC cards based on ISO/IEC7816 standard. The IC card chip 150 is a microcomputer chip embedded into a plastic plate of an IC card. An external terminal, an electrical signal protocol, and a command which the IC card chip 150 has are based on ISO/IEC7816 standard. There are a power supply terminal, a clock input terminal, a reset input terminal, an I/O input/output terminal, and a ground terminal in an external terminal of the IC card chip 150. The IC card interface control circuit 100 directs execution of an operation required for security processing demanded from the external host equipment 105 by publishing an IC card command from an external terminal of the IC card chip 150 to the IC card chip 150. The IC card chip 150 is connected with the logic channel selector 120. Composition shown in the IC card chip 150 of drawing 1 shows a logical functional block, and does not show a physical configuration.

[0011]Drawing 5 is a figure showing a physical configuration inside the IC card chip 150. The IC card chip 150, Data processing. ROM(Read Only Memory) 530 for memorizing CPU (microcomputer) 520 for carrying out, and data (a program is included), RAM(Random Access Memory) 550, EEPROM (Electrically.) It has the serial interface 570 for transmitting and receiving the code co-processor 560, and an external device and data for performing processing about Erasable Programmable ROM540, and a code/decoding. These are respectively connected by bus 580. The IC card chip 150 performs security processing corresponding to the command APDU transmitted from the host equipment 105 using the code co-processor 560. Instead of the code co-processor 560 (hardware), CPU520 may use a program (software) and may perform security processing.

[0012]The IC card chip 150 saves two or more applications in ROM530 or EEPROM540. A data area peculiar to application is secured in EEPROM530 and RAM550. As for each secured field, it is desirable to be protected by a mechanism like Fire Wall in which interference is not allowed mutually. The IC card chip 150 registers and erases application, data, and management information by the command APDU published from the IC card interface control circuit 100. As for registration of application etc., and processing of erasion, it is desirable to determine propriety of execution of the processing by access authentication. The IC card chip 150 can also have a function which chooses application by the command APDU published from the IC card interface control circuit 100.

[0013]It is desirable to carry an operating system which provides a function preselection capability of application in the IC card chip 150. As an operating system which provides such a

function, MULTOS (MULTOS is a registered trademark of Mondex International and) It is the operating system for multi-application type IC cards with which determination of specification and management of a license are performed by a MAOSCO consortium. OS etc. correspond. The operating system 130 shown in drawing 1 may provide such a function, and may not be a general-purpose operating system.

[0014]It returns to drawing 1 and explanation is continued. The operating system 130 will pass the transmitted command APDU to the application 160 chosen now, if the command APDU is received. However, in a command by which the command APDU is processed with operating systems, such as registration of application, deletion, starting, and selection, the operating system 130 performs processing corresponding to the command. The application 160 distinguishes the command APDU sent by the operating system 130, and sends it to the instruction set 161 peculiar to application, or the instruction set 143 common to application. In the instruction set 143 common to application, an instruction set including a command etc. which are needed when realizing a logical channel, a WIM instruction set, etc. correspond. As for the instruction set 161 peculiar to application, and the instruction set 143 common to application, access to EF(Elementary File)165 in which key information, certification information, etc. were stored is allowed. If the command APDU is received, the instruction set 161 peculiar to application and the instruction set 143 common to application will perform processing according to it, and will return a processing result to the host equipment 105.

[0015]The logical channel is specified in ISO/IEC 7816 and is the function to provide DF (Dedicated File) or application with an independent accessing means logically. With this function, the IC card can provide two or more services simultaneously. However, in order for an operating system to provide this function, It does not become, if the processing speed of the system by which the operating system operates, and memory space are not enough, and in the operating system used for the IC card to which the function of a system, etc. are restricted, the logical channel may not be provided as a function. MULTOSOS etc. correspond as such an operating system.

[0016]Drawing 2 is a figure showing the internal configuration of the logic channel selector 120. The logic channel selector 120 has inside of RAM221 which stored the APDU selector 210, the logical channel administrative module 220, the APDU conversion module 230, and the logical channel management table 223, and EEPROM231 which stored the APDU translation table 223. The APDU selector 210 is connected with the logical channel administrative module 220 and the APDU conversion module 230, It has the function to return the function and the response from IC card 150 which distinguish the command APDU received from the IC card interface control circuit 100, and make it process to the suitable module to the IC card interface control circuit 100. The logical channel administrative module 220 performs reservation and release of a logical channel. The logical channel number used now, the number of logical

channels opened at once, the logical channel number reserved, the application number opened now, the application executed situation, etc. are stored in RAM221 as the logical channel management table 223. The logical channel administrative module 220 processes reservation of a logical channel, etc. using the information on the logical channel management table 223 stored in RAM221. The executed situation of application is the information about which application was performed after powering on.

[0017]Inside of the command APDU to which the APDU conversion module 230 has been sent from the IC card interface control circuit 100, It has a function which complements to the command APDU to which the one or more commands APDU will have been sent if necessary in order to realize a function of a logical channel, and transmits to the IC card chip 150 about a thing about a change of application. When an error etc. occur in this sequence of a series of, the APDU conversion module 230 stops sequence processing, and tells that to the IC card interface control circuit 100. A series of sequences corresponding to the command APDU are stored in EEPROM231 as the APDU translation table 233, and the APDU conversion module 230 changes into it based on the contents of the APDU translation table 233. However, when a function of APDU conversion can be realized uniquely, it is not necessary to store these information in EEPROM231. In order to rewrite the APDU translation table 233, the command APDU for exclusive use may be prepared. Security processing of the IC card chip 150 may be used for this rewriting. The processing is directed by the command APDU of an input, and the APDU translation table 233 is rewritten by a method which the logic channel selector 120 specifies. For example, when the APDU translation table 233 takes directory structure according to the command APDU of an input, rewriting of the APDU translation table 233 is equivalent to rewriting of a corresponding directory.

[0018]Drawing 3 and drawing 4 are flow charts which show processing when access is performed from the host equipment 105 using reservation of a logical channel, and two or more logical channels. the IC card interface control circuit 100 to the command APDU -- receiving (311) -- the logic channel selector 120 judges whether the command APDU is a logical channel reservation command. A logical channel reservation command is a command for IC cards equivalent to a MANAGE CHANNELopen command in ISO/IEC7816 (331). In a logical channel reservation command, it is judged whether the logical channel administrative module 220 still has an opening in a logical channel with reference to the logical channel management table 223 (333). If a logical channel has an opening, the logic channel selector 120 will transmit a number young No. 1 except zero to the IC card interface control circuit 100 among vacant logical channels (337). When there is no vacant logical channel, the logic channel selector 120 sets that a logical channel does not open in an error signal, and transmits to the IC card interface control circuit 100 (335). The IC card interface control circuit 100 sends a received value to the host equipment 105 (313). If the command APDU is not a logical

channel reservation command, the logic channel selector 120 will judge whether it is a logical channel release command. A logical channel release command is a command for IC cards equivalent to a MANAGECHANNEL close command in ISO/IEC7816 (339). In a logical channel release command, the logic channel selector 120 judges whether a logical channel specified by the command APDU is reserved (341). When reserved, the logic channel selector 120 deletes a logical channel specified from the logical channel management table 223, and transmits to the IC card interface control circuit 100 (345). When a logical channel is not reserved, the logic channel selector 120 notifies that as an error (343). When a command differs also from reservation of a logical channel, and release, it is usually judged as a command (431).

[0019]A command in which apparatus connected is not related with a logical channel only in the case of the IC card chip 150 is transmitted to the IC card chip 150. Apparatus which operates in response to the command APDU in addition to IC card chip 150, IC card interface control circuit 100, and logic channel selector 120 in the carding machine machine 110 is carried, And when the command APDU which the logic channel selector 120 received is registered into the logic channel selector 120, the logic channel selector 120 may transmit to apparatus to which the command APDU about a future-equipment command was added. A command may usually be transmitted to added apparatus and a future-equipment command may be transmitted to the IC card chip 150. A command refers to commands other than a command about logical channel management, and a future-equipment command, and a future-equipment command usually means here a command registered into the logic channel selector 120. In a registered command, the logic channel selector 120 checks whether other apparatus is connected (449), and if it does not exist (451), that will be transmitted to the host equipment 105 (411). When other apparatus is connected, the logic channel selector 120 transmits the command APDU to the apparatus (453). If the logic channel selector 120 is contained in other apparatus at this time, the command APDU may be distributed and it may transmit to another apparatus. Also as for these apparatus, when transmitting the command APDU to other apparatus, being managed by a logical channel is desirable.

[0020]When it is not the command in which the command APDU was registered, the logic channel selector 120 judges whether it is that as which a specified logical channel is chosen now (433). When a specified logical channel is a logical channel chosen now, the logic channel selector 120 transmits the command APDU to the IC card chip 150 (435). However, an error is returned when the command APDU is already used by other logical channels with a SELECT APPLICATION command. Usually, although it is desirable not to perform simultaneously by two or more logical channels as for application, it will not be the limitation if application and host application accept this. The IC card chip 150 interprets and executes this command APDU (481). When a specified logical channel is not what is chosen now, the logic channel selector 120

judges whether specified application is chosen for the first time (437). In this case, the logic channel selector 120 transmits a SELECT APPLICATION command (439), and processing of the command APDU is performed by the IC card 150 side (483). Then, the logic channel selector 120 transmits the received command APDU to the IC card chip 150 (447), and processing of the command APDU is performed (491). When application is already chosen, The logic channel selector 120 publishes a WRITE STATIC command (441), a SELECT APPLICATION command (443), and a READ STATIC command (445) in order, and the IC card chip 150 processes these in order (485, 487, 489). A WRITE STATIC command is a command for writing in EEPROM540 temporary data which application specified now [of the IC card chip 150] holds, A READ STATIC command is a command which returns a RAM image saved with a WRITE STATIC command EEPROM540 to RAM550. However, when a command published from the IC card interface control circuit 100 is a SELECT APPLICATION command, processing of Step 447 is omitted. Although application may perform processing which corresponds to these commands before and after each command APDU processing, when this technique is used, the IC card chip 150 can be managed more efficiently. Then, the logic channel selector 120 is transmitted to the IC card chip 150 (447), and processes the received command APDU (491). It is not transmitted to the IC card interface control circuit 100, but a response about commands APDU other than the command APDU received from the IC card interface control circuit 100 is processed by the logic channel selector 120. When an error occurs, if the logic channel selector 120 is necessary, after it will change, it returns an error code generated inside to the IC card interface control circuit 100 as a response of the received command APDU.

[0021]A position of the logic channel selector 120 is not restricted between the IC card chip 150 and the IC card interface control circuit 100. The logic channel selector 120 can be arranged at arbitrary places of as [which is the command APDU / whose an output is the command APDU], although command formats differ, when compatible, may change a command format and may be used. A card reader writer etc. which change a communications protocol or connector form where this place is inserted between the host equipment 105 and the carding machine machine 110 in the host equipment 105 etc. correspond. It is desirable to install the logic channel selector 120 in the host equipment 105 to manage two or more carding machine machines 110 by a logical channel.

[0022]Usually, although application stored in the IC card chip 150 is independently accessed with an external instrument using a logical channel, there is a case where he would like to perform data communications between applications, without taking out data to the exterior of the IC card chip 150 which is the Tampa-proof field. Processing of payment of electronic money, payment, etc. in which this was specifically stored in application with a function of an electronic purse corresponds.

[0023]Drawing 6 is a flow chart at the time of realizing processing mentioned above. Hereafter, it explains, also quoting the description of drawing 1. When the logical channel different from the logical channel chosen in Step 433 of drawing 4 now is chosen, as for the logic channel selector 120, it is judged next whether it is selection of registration application (611). When it is not selection of registration application, a 437 or less-step step is performed. In the case of registration application, the logic channel selector 120 publishes a false application selection command to the application 160 chosen now [of the IC card chip 150] (613). A false application selection command is a command which changes the application selection command (it is equivalent to the SELECT APPLICATION command in ISO/IEC 7816) published by the host into the form which each application in the IC card chip 150 understands. As for an application selection command, in the usual use, it is desirable for the system each application controls application like an operating system rather than processes to receive and perform. However, it is better for an application selection command to make an operating system bypass, and to be able to transmit to application, when performing an internal call of application. This invention provides this function.

[0024]If this command is received, the application 160 will be changed into the inside call instruction of application, and will call the application 190 (651). The called application 190 judges whether it is having acted the internal call as oneself (681). In the call from an inside, APDU processing for an internal call is performed (683), and, in the call from the outside, APDU processing for an external call is performed (685). It judges whether its call is a call from an inside, and whether the application 190 is the call from the outside (operating system 130), and has a function which divides processing. It is judged to a false application selection command whether this is received or not. With this function, it is decided how it communicates between applications. For example, as for the usual application, it is desirable to be set up not receive invoking. As for application like electronic money, it is desirable to be set up so that it may be called only from the application registered into electronic money application.

[0025]Via the application 160, it is transmitted to the application 190 and the usual command (615) below a false application selection command is processed (687). (653) Specifically, the format of the sent usual command is changed and called using an internal call instruction. The internal call is valid until other applications are chosen. The host equipment 105 may publish the command APDU which performs one or two or more processings between the application 160 and the application 190 ignited by a false application selection command. The operation etc. which purchase goods, such as attestation between applications and an electronic ticket which used electronic money, correspond to this.

[0026]By the case where an application selection command is published, when the selected application is the application by the side of a call (617), a RETURN command is published (619). The call side application ends invoking, taking advantage of this opportunity, and the

command received henceforth processes it as a command for application 160. When other applications are chosen (621), Transmit a RETURN command (623) and a call is ended (657), Next, it processes by publishing a WRITE STATIC command (625), a SELECT APPLICATION command (627), and a READ STATIC command (619) in order (659, 661, 689). Processing of a call may become an embedded structure. In [and capacity of RAM cannot fully secure by restrictions of the operating system 130 and the IC card chip 150 in that case] the time of an application change, In the case of the temporary data and the register about the before selected application not being held. Before calling application, these data is evacuated to EEPROM540, and the temporary data and the register which were evacuated to EEPROM540 are restored after the re-call of application. However, when the internal call is not accepted in the specified application, internal call processing cannot be performed but it is processed as an external call. At this time, an external call may not be performed but an error may be returned. [0027]A function of a logical channel is applicable besides IC card chip 150. Other systems using a support of MultiMediaCard ("MultiMediaCard" is a registered trademark of InfineonTechnologiesAG) or a logical channel correspond to this. A format of a command which is sent to the logic channel selector 120 and the logic channel selector 120 publishes when not using the IC card chip 150 as one of the devices, It may use except a command APDU format of a command for IC cards specified by ISO/IEC7816. However, if a command set has a command for IC cards, and compatibility and it has a command format convertible into an IC card command and a response, The IC card chip 150 can also be used by inserting command conversion equipment between the logic channel selector 120 and the IC card chip 150. When performing common processing in two or more applications, such as a command about the APDU selection modules 140 and 192 and a logical channel, a system applicable to the operating system 130 may mount this function.

[0028]Drawing 7 is a figure showing the example which serves WAP (Wireless Application Protocol) using the carding machine machines 710, such as the host equipment 105, such as a personal digital assistant, and a SIM card. The carding machine machine 710 operates as WIM (WAP Identity Module) which performs security processing. WAP is the specification defined in WAP forum for the application which gives its service on a wireless communication network, and is the specification defined for the application which performs security processing on WAP in WIM. The application 760 in the IC card chip 150, It has the function to perform WIM application and this is divided into the command 743 for WIM, an application selection related command, and the application command 161 with the APDU selection module 140 in the application 760. However, an application selection related command shall be included as an extended set of the command 743 for WIM. When application 790 is made into the application for electronic money, the application 790, As opposed to other application 770 grades registered into the application 790, It has a function which fluctuates the electronic money data

stored in EEPROM in the application 790, It has a function in which the contractor who had a function saved at the above-mentioned EEPROM by making into a log the exchange performed at this time, and published applications 790, such as a bank, performs reading and elimination for the above-mentioned log, and a function which fluctuates electronic money data. It can process by using an internal call of application, without taking out confidential information, such as electronic money data, outside.

[0029]Drawing 8 is a figure showing the case where carry the IC card chip 150 and the flash memory chip 860 in MultiMediaCard(following MMC) 820, and these are controlled by the logic channel selector 120. The controller chip 850, The MMC external terminal 830. The MMC interface control circuit 853 to control, the IC card interface control circuit 100 which performs control of the IC card chip 150, the flash memory control circuit 855 which performs control of the flash memory chip 160, the logic channel selector 120, and these. The controller module 857 to control is comprised. The flash memory chip 860 is a memory chip which uses nonvolatile semiconductor memory as a storage, and reading and writing of data are made by a flash plate memory command. The MMC external terminal 830 comprises seven terminals, and in order to exchange information with the external host equipment 105, it contains a power supply terminal, a clock input terminal, a command input/output terminal, a data input/output terminal, and a ground terminal. It has a logical channel for one or more flash memories, and a logical channel for other IC cards, they are changed by the logic channel selector 120, and the host equipment 105 is sent to each controller. By using this structure, application which cooperates mutually-independent and performs access of a flash memory and an IC card is realized. The structure of access to the IC card chip 150 and access to the flash memory chip 860 can be communalized according to this structure. This structure is effective also when taking the composition which includes the IC card chip 150 in the controller chip 850.

[0030]

[Effect of the Invention]According to this invention, the effect of improving the convenience of an IC card can be done so by giving the function of a logical channel to the operating system for an IC card and IC cards which does not support a logical channel.

CLAIMS

[Claim(s)]

[Claim 1]Memory storage comprising:

The 1st memory that performs security processing of data.

A control device which controls said 1st memory.

The 2nd memory that gives a function of a logical channel to said 1st memory.

[Claim 2]The memory storage comprising according to claim 1:

A means by which said 2nd memory performs processing corresponding to a command about said logical channel when a command about a logical channel is included in a command from host equipment connected to this memory storage.

A means to complement conversion of a command received from said host equipment and one, or two or more commands, and to transmit to said 1st memory.

[Claim 3]The memory storage comprising according to claim 1:

A means to perform processing corresponding to a command about said logical channel when it has the 3rd memory corresponding to a command of a different system from a command inputted into said 1st memory and a command about a logical channel is included in a command from host equipment by which said 2nd memory is connected to this memory storage.

A means to complement conversion of a command received from said host equipment and one, or two or more commands, and to transmit to said 3rd memory.

[Claim 4]The memory storage comprising according to claim 2:

The 1st command that writes data which said 2nd memory has RAM and EEPROM, and was stored in said RAM in said EEPROM.

The 2nd command that returns data written in said EEPROM by said 1st command to said RAM.

A means to perform processing of said logical channel using the 3rd command that changes application with an operating system.

[Claim 5]The memory storage comprising according to claim 4:

The 1st module in which said 2nd memory has been sent from said host equipment when a command about registration application is included in a command from said host equipment and that usually changes a command into a pseudo-instruction.

The 2nd module that changes into a false application selection command and a false

application selection end instruction an application selection command sent from said host equipment.

[Claim 6]As opposed to the 1st application with which said false application selection command was stored in said 1st memory, It is the command which performs an internal call of the 2nd application stored in said 1st memory specified with said false application selection command, The memory storage according to claim 5, wherein said false application selection end instruction is a command which terminates an internal call of said 2nd application to said 1st application.

[Claim 7]A means to judge that to which said 1st application was transmitted from what was transmitted from other applications with which a command was stored in said 1st memory, and the 2nd memory, The memory storage according to claim 6 having a means to process a command received from said 2nd memory, and a means to process a command received from application of others in said 1st memory.

[Claim 8]The memory storage according to claim 7, wherein said 1st application has a means to change into one or two or more commands a command received from said 2nd memory, and to transmit to said 2nd application.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the host equipment in which the host equipment which can insert the memory storage which has a security function, and its memory storage, and memory storage were inserted, It is related with the terminal unit with which the host device which can insert the memory storage which has a controller which manages a logical channel especially, and its memory storage, and its memory storage were inserted.

PRIOR ART

[Description of the Prior Art]An IC card embeds IC (integrated circuit) chip into a plastic card board, and has an external terminal of an IC chip in the card-face side. A power supply terminal, a clock terminal, a data input/output terminal, etc. are contained in the external terminal of an IC chip. The IC card operates by carrying out direct supply of a power supply or the driving clock via an external terminal from the host device connected with an IC card. An IC card exchanges information with the connected host equipment by transmitting and receiving an electrical signal between host equipment via an external terminal. As a result of information exchange, an IC card performs sending out of a calculation result or memory information, and change of memory information. The IC card can have the function to perform security processings, such as security data protection and personal authentication, based on such operation specifications. In the system for which the security of extra sensitive information, such as credit settlement and banking, is needed, the IC card is used as a user device for identification.

EFFECT OF THE INVENTION

[Effect of the Invention]According to this invention, the effect of improving the convenience of an IC card can be done so by giving the function of a logical channel to the operating system for an IC card and IC cards which does not support a logical channel.

TECHNICAL PROBLEM

[Problem to be solved by the invention]An IC card which is not supporting a logical channel when two or more applications are carried in IC card chip. Or in an IC card which carries an operating system for IC cards which is not supporting a logical channel, it is difficult to make two or more applications cooperate and to operate them independently, simultaneously.

[0004]Although it is also possible to use commands other than a command specified by ISO/IEC7816, a command to an IC card, If a command which is not specified by ISO/IEC7816 is used when OS in an IC card operates a system of a logical channel, only application in an IC card can be operated in a logical channel which is a system which can operate two or more devices simultaneously.

[0005]The purpose of this invention is to operate simultaneously independently two or more applications carried in an IC card, and is improving the convenience of an IC card.

MEANS

[Means for solving problem] In order to attain the above-mentioned purpose, let this inventions be the 1st memory that performs security processing of data, a control device which controls the 1st memory, and the memory storage which has the 2nd memory that gives the function of a logical channel to memory storage.

[0007] The 2nd memory may perform processing of a logical channel, when the command about a logical channel is included in the command from the host equipment connected to memory storage.

[0008] The 2nd memory is good also as composition which has RAM and ROM. In this case, the command by which the 2nd memory writes RAM data in EEPROM, processing of a logical channel may be performed using the command which returns the data written in EEPROM to RAM, and the command which changes application with an operating system -- to a pan the 2nd memory, The module which has been sent from host equipment when the command about registration application is included in the command from host equipment and which usually changes a command into a pseudo-instruction, It may have a module which changes into a false application selection command and a false application selection end instruction the application selection command sent from host equipment.

[0009] The application stored in the 1st memory, A means by which a command judges what has been sent from other applications stored in the 1st memory, and the thing sent from the 2nd memory, It may have a means to process the command sent from other applications, and a means to process the command sent from the 2nd memory.

[0010]

[Invention embodiment] Drawing 1 is a figure showing the composition of the carding machine machine 110 which applied this invention. The carding machine machine 110 comprises the IC card interface control circuit 100, the logic channel selector 120, and the IC card chip 150. The IC card interface control circuit 100 controls the IC card chip 150, and controls transmission and reception of the command APDU between the host equipment 105 and the logic channel selector 120. The logic channel selector 120 is connected to the IC card chip 150 and the IC card interface control circuit 100, A logical channel controlling function is provided to the operating system for an IC card and IC cards which is not supporting the logical channel, and a command is distributed to other apparatus which receives the command APDU. A flash memory chip, RAM, etc. correspond with other apparatus here. After the command APDU corresponding to these apparatus changes the command APDU received when necessary, it is handed over by the controller which controls these apparatus. The command APDU is the command format and the command for IC cards for IC cards based on ISO/IEC7816 standard. The IC card chip 150 is a microcomputer chip embedded into the plastic plate of an IC card.

The external terminal, electrical signal protocol, and command which the IC card chip 150 has are based on ISO/IEC7816 standard. There are a power supply terminal, a clock input terminal, a reset input terminal, an I/O input/output terminal, and a ground terminal in the external terminal of the IC card chip 150. The IC card interface control circuit 100 directs execution of an operation required for the security processing demanded from the external host equipment 105 by publishing an IC card command from the external terminal of the IC card chip 150 to the IC card chip 150. The IC card chip 150 is connected with the logic channel selector 120. The composition shown in the IC card chip 150 of drawing 1 shows a logical functional block, and does not show a physical configuration.

[0011]Drawing 5 is a figure showing a physical configuration inside the IC card chip 150. The IC card chip 150, Data processing. ROM(Read Only Memory) 530 for memorizing CPU (microcomputer) 520 for carrying out, and data (a program is included), RAM(Random Access Memory) 550, EEPROM (Electrically.) It has the serial interface 570 for transmitting and receiving the code co-processor 560, and an external device and data for performing processing about Erasable Programmable ROM540, and a code/decoding. These are respectively connected by bus 580. The IC card chip 150 performs security processing corresponding to the command APDU transmitted from the host equipment 105 using the code co-processor 560. Instead of the code co-processor 560 (hardware), CPU520 may use a program (software) and may perform security processing.

[0012]The IC card chip 150 saves two or more applications in ROM530 or EEPROM540. A data area peculiar to application is secured in EEPROM530 and RAM550. As for each secured field, it is desirable to be protected by a mechanism like Fire Wall in which interference is not allowed mutually. The IC card chip 150 registers and erases application, data, and management information by the command APDU published from the IC card interface control circuit 100. As for registration of application etc., and processing of erasion, it is desirable to determine propriety of execution of the processing by access authentication. The IC card chip 150 can also have a function which chooses application by the command APDU published from the IC card interface control circuit 100.

[0013]It is desirable to carry the operating system which provides the function preselection capability of application in the IC card chip 150. As an operating system which provides such a function, MULTOS (MULTOS is a registered trademark of Mondex International and) It is the operating system for multi-application type IC cards with which determination of specification and management of the license are performed by the MAOSCO consortium. OS etc. correspond. The operating system 130 shown in drawing 1 may provide such a function, and may not be a general-purpose operating system.

[0014]It returns to drawing 1 and explanation is continued. The operating system 130 will pass the transmitted command APDU to the application 160 chosen now, if the command APDU is

received. However, in the command by which the command APDU is processed with operating systems, such as registration of application, deletion, starting, and selection, the operating system 130 performs processing corresponding to the command. The application 160 distinguishes the command APDU sent by the operating system 130, and sends it to the instruction set 161 peculiar to application, or the instruction set 143 common to application. In the instruction set 143 common to application, an instruction set including the command etc. which are needed when realizing a logical channel, a WIM instruction set, etc. correspond. As for the instruction set 161 peculiar to application, and the instruction set 143 common to application, access to EF(Elementary File)165 in which key information, certification information, etc. were stored is allowed. If the command APDU is received, the instruction set 161 peculiar to application and the instruction set 143 common to application will perform processing according to it, and will return a processing result to the host equipment 105. [0015]A logical channel is specified in ISO/IEC 7816 and is the function to provide DF (Dedicated File) or application with an independent accessing means logically. With this function, the IC card can provide two or more services simultaneously. However, in order for an operating system to provide this function, It does not become, if processing speed of a system by which the operating system operates, and memory space are not enough, and in an operating system used for an IC card to which a function of a system, etc. are restricted, a logical channel may not be provided as a function. MULTOSOS etc. correspond as such an operating system.

[0016]Drawing 2 is a figure showing an internal configuration of the logic channel selector 120. The logic channel selector 120 has inside of RAM221 which stored the APDU selector 210, the logical channel administrative module 220, the APDU conversion module 230, and the logical channel management table 223, and EEPROM231 which stored the APDU translation table 223. The APDU selector 210 is connected with the logical channel administrative module 220 and the APDU conversion module 230, It has the function to return a function and a response from IC card 150 which distinguish the command APDU received from the IC card interface control circuit 100, and make it process to a suitable module to the IC card interface control circuit 100. The logical channel administrative module 220 performs reservation and release of a logical channel. A logical channel number used now, the number of logical channels opened at once, a logical channel number reserved, an application number opened now, an application executed situation, etc. are stored in RAM221 as the logical channel management table 223. The logical channel administrative module 220 processes reservation of a logical channel, etc. using information on the logical channel management table 223 stored in RAM221. An executed situation of application is the information about which application was performed after powering on.

[0017]Inside of the command APDU to which the APDU conversion module 230 has been sent

from the IC card interface control circuit 100, It has a function which complements to the command APDU to which the one or more commands APDU will have been sent if necessary in order to realize a function of a logical channel, and transmits to the IC card chip 150 about a thing about a change of application. When an error etc. occur in this sequence of a series of, the APDU conversion module 230 stops sequence processing, and tells that to the IC card interface control circuit 100. A series of sequences corresponding to the command APDU are stored in EEPROM231 as the APDU translation table 233, and the APDU conversion module 230 changes into it based on the contents of the APDU translation table 233. However, when a function of APDU conversion can be realized uniquely, it is not necessary to store these information in EEPROM231. In order to rewrite the APDU translation table 233, the command APDU for exclusive use may be prepared. Security processing of the IC card chip 150 may be used for this rewriting. The processing is directed by the command APDU of an input, and the APDU translation table 233 is rewritten by a method which the logic channel selector 120 specifies. For example, when the APDU translation table 233 takes directory structure according to the command APDU of an input, rewriting of the APDU translation table 233 is equivalent to rewriting of a corresponding directory.

[0018]Drawing 3 and drawing 4 are flow charts which show processing when access is performed from the host equipment 105 using reservation of a logical channel, and two or more logical channels. the IC card interface control circuit 100 to the command APDU -- receiving (311) -- the logic channel selector 120 judges whether the command APDU is a logical channel reservation command. A logical channel reservation command is a command for IC cards equivalent to the MANAGE CHANNELopen command in ISO/IEC7816 (331). In a logical channel reservation command, it is judged whether the logical channel administrative module 220 still has an opening in a logical channel with reference to the logical channel management table 223 (333). If a logical channel has an opening, the logic channel selector 120 will transmit the number young No. 1 except zero to the IC card interface control circuit 100 among vacant logical channels (337). When there is no vacant logical channel, the logic channel selector 120 sets that a logical channel does not open in an error signal, and transmits to the IC card interface control circuit 100 (335). The IC card interface control circuit 100 sends the received value to the host equipment 105 (313). If the command APDU is not a logical channel reservation command, the logic channel selector 120 will judge whether it is a logical channel release command. A logical channel release command is a command for IC cards equivalent to the MANAGECHANNEL close command in ISO/IEC7816 (339). In a logical channel release command, the logic channel selector 120 judges whether the logical channel specified by the command APDU is reserved (341). When reserved, the logic channel selector 120 deletes the logical channel specified from the logical channel management table 223, and transmits to the IC card interface control circuit 100 (345). When the logical channel is not

reserved, the logic channel selector 120 notifies that as an error (343). When a command differs also from reservation of a logical channel, and release, it is usually judged as a command (431).

[0019]The command in which the apparatus connected is not related with a logical channel only in the case of the IC card chip 150 is transmitted to the IC card chip 150. The apparatus which operates in response to the command APDU in addition to IC card chip 150, IC card interface control circuit 100, and logic channel selector 120 in the carding machine machine 110 is carried, And when the command APDU which the logic channel selector 120 received is registered into the logic channel selector 120, the logic channel selector 120 may transmit to the apparatus to which the command APDU about a future-equipment command was added. A command may usually be transmitted to the added apparatus and a future-equipment command may be transmitted to the IC card chip 150. A command refers to commands other than the command about logical channel management, and a future-equipment command, and a future-equipment command usually means here the command registered into the logic channel selector 120. In the registered command, the logic channel selector 120 checks whether other apparatus is connected (449), and if it does not exist (451), that will be transmitted to the host equipment 105 (411). When other apparatus is connected, the logic channel selector 120 transmits the command APDU to the apparatus (453). If the logic channel selector 120 is contained in other apparatus at this time, the command APDU may be distributed and it may transmit to another apparatus. Also as for these apparatus, when transmitting the command APDU to other apparatus, being managed by the logical channel is desirable.

[0020]When it is not the command in which the command APDU was registered, the logic channel selector 120 judges whether it is that as which the specified logical channel is chosen now (433). When the specified logical channel is a logical channel chosen now, the logic channel selector 120 transmits the command APDU to the IC card chip 150 (435). However, an error is returned when the command APDU is already used by other logical channels with a SELECT APPLICATION command. Usually, although it is desirable not to perform simultaneously by two or more logical channels as for application, it will not be the limitation if application and host application accept this. The IC card chip 150 interprets and executes this command APDU (481). When the specified logical channel is not what is chosen now, the logic channel selector 120 judges whether the specified application is chosen for the first time (437). In this case, the logic channel selector 120 transmits a SELECT APPLICATION command (439), and processing of the command APDU is performed by the IC card 150 side (483). Then, the logic channel selector 120 transmits the received command APDU to the IC card chip 150 (447), and processing of the command APDU is performed (491). When application is already chosen, The logic channel selector 120 publishes a WRITE STATIC command (441), a

SELECT APPLICATION command (443), and a READ STATIC command (445) in order, and the IC card chip 150 processes these in order (485, 487, 489). A WRITE STATIC command is a command for writing in EEPROM540 the temporary data which the application specified now [of the IC card chip 150] holds, A READ STATIC command is a command which returns the RAM image saved with a WRITE STATIC command EEPROM540 to RAM550. However, when the command published from the IC card interface control circuit 100 is a SELECT APPLICATION command, processing of Step 447 is omitted. Although application may perform processing which corresponds to these commands before and after each command APDU processing, when this technique is used, the IC card chip 150 can be managed more efficiently. Then, the logic channel selector 120 is transmitted to the IC card chip 150 (447), and processes the received command APDU (491). It is not transmitted to the IC card interface control circuit 100, but the response about commands APDU other than the command APDU received from the IC card interface control circuit 100 is processed by the logic channel selector 120. When an error occurs, if the logic channel selector 120 is necessary, after it will change, it returns the error code generated inside to the IC card interface control circuit 100 as a response of the received command APDU.

[0021]A position of the logic channel selector 120 is not restricted between the IC card chip 150 and the IC card interface control circuit 100. The logic channel selector 120 can be arranged at arbitrary places of as [which is the command APDU / whose an output is the command APDU], although command formats differ, when compatible, may change a command format and may be used. A card reader writer etc. which change a communications protocol or connector form where this place is inserted between the host equipment 105 and the carding machine machine 110 in the host equipment 105 etc. correspond. It is desirable to install the logic channel selector 120 in the host equipment 105 to manage two or more carding machine machines 110 by a logical channel.

[0022]Usually, although application stored in the IC card chip 150 is independently accessed with an external instrument using a logical channel, there is a case where he would like to perform data communications between applications, without taking out data to the exterior of the IC card chip 150 which is the Tampa-proof field. Processing of payment of electronic money, payment, etc. in which this was specifically stored in application with a function of an electronic purse corresponds.

[0023]Drawing 6 is a flow chart at the time of realizing processing mentioned above. Hereafter, it explains, also quoting the description of drawing 1. When the logical channel different from the logical channel chosen in Step 433 of drawing 4 now is chosen, as for the logic channel selector 120, it is judged next whether it is selection of registration application (611). When it is not selection of registration application, a 437 or less-step step is performed. In the case of registration application, the logic channel selector 120 publishes a false application selection

command to the application 160 chosen now [of the IC card chip 150] (613). A false application selection command is a command which changes the application selection command (it is equivalent to the SELECT APPLICATION command in ISO/IEC 7816) published by the host into the form which each application in the IC card chip 150 understands. As for an application selection command, in the usual use, it is desirable for the system each application controls application like an operating system rather than processes to receive and perform. However, it is better for an application selection command to make an operating system bypass, and to be able to transmit to application, when performing an internal call of application. This invention provides this function.

[0024]If this command is received, the application 160 will be changed into an inside call instruction of application, and will call the application 190 (651). The called application 190 judges whether it is having acted an internal call as oneself (681). In a call from an inside, APDU processing for an internal call is performed (683), and, in a call from the outside, APDU processing for an external call is performed (685). It judges whether its call is a call from an inside, and whether the application 190 is the call from the outside (operating system 130), and has a function which divides processing. It is judged to a false application selection command whether this is received or not. With this function, it is decided how it communicates between applications. For example, as for the usual application, it is desirable to be set up not receive invoking. As for application like electronic money, it is desirable to be set up so that it may be called only from application registered into electronic money application.

[0025]Via the application 160, it is transmitted to the application 190 and a usual command (615) below a false application selection command is processed (687). (653) Specifically, a format of a sent usual command is changed and called using an internal call instruction. An internal call is valid until other applications are chosen. The host equipment 105 may publish the command APDU which performs one or two or more processings between the application 160 and the application 190 ignited by a false application selection command. Operation etc. which purchase goods, such as attestation between applications and an electronic ticket which used electronic money, correspond to this.

[0026]By the case where an application selection command is published, when the selected application is the application by the side of a call (617), a RETURN command is published (619). The call side application ends invoking, taking advantage of this opportunity, and the command received henceforth processes it as a command for application 160. When other applications are chosen (621), Transmit a RETURN command (623) and a call is ended (657), Next, it processes by publishing a WRITE STATIC command (625), a SELECT APPLICATION command (627), and a READ STATIC command (619) in order (659, 661, 689). Processing of a call may become an embedded structure. In [and capacity of RAM cannot fully secure by restrictions of the operating system 130 and the IC card chip 150 in that case] the time of an

application change, In the case of the temporary data and the register about the before selected application not being held. Before calling application, these data is evacuated to EEPROM540, and the temporary data and the register which were evacuated to EEPROM540 are restored after the re-call of application. However, when the internal call is not accepted in the specified application, internal call processing cannot be performed but it is processed as an external call. At this time, an external call may not be performed but an error may be returned. [0027]A function of a logical channel is applicable besides IC card chip 150. Other systems using a support of MultiMediaCard ("MultiMediaCard" is a registered trademark of InfineonTechnologiesAG) or a logical channel correspond to this. A format of a command which is sent to the logic channel selector 120 and the logic channel selector 120 publishes when not using the IC card chip 150 as one of the devices, It may use except a command APDU format of a command for IC cards specified by ISO/IEC7816. However, if a command set has a command for IC cards, and compatibility and it has a command format convertible into an IC card command and a response, The IC card chip 150 can also be used by inserting command conversion equipment between the logic channel selector 120 and the IC card chip 150. When performing common processing in two or more applications, such as a command about the APDU selection modules 140 and 192 and a logical channel, a system applicable to the operating system 130 may mount this function.

[0028]Drawing 7 is a figure showing the example which serves WAP (Wireless Application Protocol) using the carding machine machines 710, such as the host equipment 105, such as a personal digital assistant, and a SIM card. The carding machine machine 710 operates as WIM (WAP Identity Module) which performs security processing. WAP is the specification defined in WAP forum for the application which gives its service on a wireless communication network, and is the specification defined for the application which performs security processing on WAP in WIM. The application 760 in the IC card chip 150, It has the function to perform WIM application and this is divided into the command 743 for WIM, an application selection related command, and the application command 161 with the APDU selection module 140 in the application 760. However, an application selection related command shall be included as an extended set of the command 743 for WIM. When application 790 is made into the application for electronic money, the application 790, As opposed to other application 770 grades registered into the application 790, It has a function which fluctuates the electronic money data stored in EEPROM in the application 790, It has a function in which the contractor who had a function saved at the above-mentioned EEPROM by making into a log the exchange performed at this time, and published applications 790, such as a bank, performs reading and elimination for the above-mentioned log, and a function which fluctuates electronic money data. It can process by using an internal call of application, without taking out confidential information, such as electronic money data, outside.

[0029]Drawing 8 is a figure showing a case where carry the IC card chip 150 and the flash memory chip 860 in MultiMediaCard(following MMC) 820, and these are controlled by the logic channel selector 120. The controller chip 850, The MMC external terminal 830. The MMC interface control circuit 853 to control, the IC card interface control circuit 100 which performs control of the IC card chip 150, the flash memory control circuit 855 which performs control of the flash memory chip 160, the logic channel selector 120, and these. The controller module 857 to control is comprised. The flash memory chip 860 is a memory chip which uses nonvolatile semiconductor memory as a storage, and reading and writing of data are made by a flash plate memory command. The MMC external terminal 830 comprises seven terminals, and in order to exchange information with the external host equipment 105, it contains a power supply terminal, a clock input terminal, a command input/output terminal, a data input/output terminal, and a ground terminal. It has a logical channel for one or more flash memories, and a logical channel for other IC cards, they are changed by the logic channel selector 120, and the host equipment 105 is sent to each controller. By using this structure, application which cooperates mutually-independent and performs access of a flash memory and an IC card is realized. Structure of access to the IC card chip 150 and access to the flash memory chip 860 can be communalized according to this structure. This structure is effective also when taking composition which includes the IC card chip 150 in the controller chip 850.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a figure showing the internal configuration of the carding machine machine which has IC card chip.

[Drawing 2] It is a figure showing the internal configuration of a logic channel selector.

[Drawing 3] It is a flow chart which shows the procedure of logical channel management.

[Drawing 4] It is a flow chart which shows the procedure of logical channel management.

[Drawing 5] It is a figure showing the internal configuration of IC card chip.

[Drawing 6] It is a flow chart at the time of performing an internal call of application.

[Drawing 7] It is a figure showing the internal configuration at the time of serving WAP using the carding machine machine which has IC card chip.

[Drawing 8] It is a figure showing the case where a logic channel selector is carried in MMC which has IC card chip.

[Explanations of letters or numerals]

105 [-- IC card chip.] -- Host equipment, 100 -- An IC card interface control circuit, 120 -- A logic channel selector, 150